

Amendments to the Claims

Please add new claims 23-24 as indicated below. All claims are listed below, with new claims so marked. This listing of claims will replace all prior versions, and listings, of claims in the application:

1 1. (Original) A method for de-authenticating from a first web server
2 security realm protected by an authentication scheme lacking a de-authentication
3 operation, the method comprising:
4 attempting to access a first resource in a first security realm protected by the
5 authentication scheme;
6 receiving a request for authentication credentials in response to said attempting
7 to access the first resource;
8 supplying said authentication credentials in response to the request so as to
9 become authenticated in the first security realm; and
10 accessing a logout resource in the first security realm, said logout resource
11 configured to automatically authenticate with a second security realm on accessing
12 thereof.

1 2. (Original) The method of claim 1, further comprising:
2 providing a common access point executing a web browser;
3 first displaying a login web page of the second security realm so that a first user
4 may authenticate with the first security realm and access the first resource, the login
5 page comprising a login resource configured to perform said attempting to access the
6 first resource; and

7 second displaying the login web page of the second security realm responsive to
8 said accessing the logout resource so that a second user may authenticate with the first
9 security realm and access the first resource.

1 3. (Original) The method of claim 1, wherein the logout resource
2 executes a script configured to authenticate a user with the second security realm.

1 4. (Original) The method of claim 3, wherein the logout resource
2 comprises a web page element comprising a link to the script, and wherein the web
3 page element incorporates authentication credentials for the second security realm so
4 that the user need not provide authentication credentials to access the second security
5 realm.

1 5. (Original) The method of claim 1, wherein the authentication scheme
2 comprises HTTP basic authentication.

1 6. (Original) A method for de-authenticating from an HTTP basic
2 authentication, comprising:
3 attempting to access a first resource in a first security realm protected by HTTP
4 basic authentication;
5 responsive to said attempting to access, receiving an authentication request for
6 controlling access to the first resource;
7 supplying authentication credentials responsive to said authentication request so
8 as to authenticate with the first security realm;
9 accessing a second resource in the first security realm; and

10 responsive to said accessing the second resource, automatically authenticating
11 with a second security realm.

1 7. (Original) The method of claim 6, wherein said authenticating with the
2 second security realm invalidates a prior authentication with the first security realm.

1 8. (Original) The method of claim 7, further comprising:
2 displaying a login element within a web browser, the login element configured to
3 access the first resource upon activation thereof.

1 9. (Original) The method of claim 8, further comprising:
2 displaying a logout element within the web browser for performing said
3 automatically authenticating with the second security realm; and
4 within a single browser session:
5 authenticating a first user with the first security realm;
6 authenticating the first user with the second security realm so as to de-
7 authenticate the first user from the first security realm; and
8 authenticating a second user with the first security realm.

1 10. (Original) An article of manufacture for de-authenticating from a first
2 web server security realm protected by an authentication scheme lacking a de-
3 authentication operation, comprising a readable medium having instructions encoded
4 thereon for execution by a processor, said instructions capable of directing the
5 processor to perform:

6 attempting to access a first resource in a first security realm protected by the
7 authentication scheme;

8 receiving a request for authentication credentials in response to said attempting
9 to access the first resource;

10 supplying said authentication credentials in response to the request so as to
11 become authenticated in the first security realm; and

12 accessing a logout resource in the first security realm, said logout resource
13 configured to automatically authenticate with a second security realm on accessing
14 thereof.

1 11. (Original) The article of manufacture of claim 10, said instructions
2 comprising further instructions capable of directing the processor to perform:

3 providing a common access point executing a web browser;

4 first displaying a login web page of the second security realm so that a first user
5 may authenticate with the first security realm and access the first resource, the login
6 page comprising a login resource configured to perform said attempting to access the
7 first resource; and

8 second displaying the login web page of the second security realm responsive to
9 said accessing the logout resource so that a second user may authenticate with the first
10 security realm and access the first resource.

1 12. (Original) The article of manufacture of claim 10, wherein said
2 instructions for said logout resource comprise instructions capable of directing the

processor to execute a script configured to authenticate a user with the second security realm.

13. (Original) The article of manufacture of claim 12, further comprising:
said instructions for said logout resource further comprising instructions capable
of directing the processor to provide a web page element comprising a link to the script;
and
said instructions for said web page element further comprising instructions
capable of directing the processor to provide authentication credentials for the second
security realm so that the user need not provide authentication credentials to access the
second security realm.

14. (Original) The article of manufacture of claim 10, wherein the
authentication scheme comprises HTTP basic authentication.

15. (Original) An article of manufacture for de-authenticating from an
HTTP basic authentication comprising a readable medium having instructions encoded
thereon for execution by a processor, said instructions capable of directing the
processor to perform:
attempting to access a first resource in a first security realm protected by HTTP
basic authentication;
responsive to said attempting to access, receiving an authentication request for
controlling access to the first resource;

9 supplying authentication credentials responsive to said authentication request so
10 as to authenticate with the first security realm;
11 accessing a second resource in the first security realm; and
12 responsive to said accessing the second resource, automatically authenticating
13 with a second security realm.

1 16. (Original) The article of manufacture of claim 15, wherein said
2 instructions for authenticating with the second security realm invalidates a prior
3 authentication with the first security realm.

1 17. (Original) The article of manufacture of claim 16, said instructions
2 comprising further instructions capable of directing the processor to perform:
3 displaying a login element within a web browser, the login element configured to
4 access the first resource upon activation thereof.

1 18. (Original) The article of manufacture of claim 17, said instructions
2 comprising further instructions capable of directing the processor to perform:
3 displaying a logout element within the web browser for performing said
4 automatically authenticating with the second security realm; and
5 within a single browser session:
6 authenticating a first user with the first security realm;
7 authenticating the first user with the second security realm so as to de-
8 authenticate the first user from the first security realm; and
9 authenticating a second user with the first security realm.

1 19. (Original) An apparatus for de-authenticating from a first web server
2 security realm protected by an authentication scheme lacking a de-authentication
3 operation, comprising:

4 means for attempting to access a first resource in a first security realm protected
5 by the authentication scheme;

6 means for receiving a request for authentication credentials in response to said
7 attempting to access the first resource;

8 means for supplying said authentication credentials in response to the request so
9 as to become authenticated in the first security realm; and

10 means for accessing a logout resource in the first security realm, said logout
11 resource configured to automatically authenticate with a second security realm on
12 accessing thereof.

1 20. (Original) The apparatus of claim 10, further comprising:

2 means for providing a common access point executing a web browser;

3 means for first displaying a login web page of the second security realm so that a
4 first user may authenticate with the first security realm and access the first resource, the
5 login page comprising a login resource configured to perform said attempting to access
6 the first resource; and

7 means for second displaying the login web page of the second security realm
8 responsive to said accessing the logout resource so that a second user may
9 authenticate with the first security realm and access the first resource.

1 21. (Original) An apparatus for de-authenticating from an HTTP basic
2 authentication comprising:
3 means for attempting to access a first resource in a first security realm protected
4 by HTTP basic authentication;
5 responsive to said attempting to access, means for receiving an authentication
6 request for controlling access to the first resource;
7 means for supplying authentication credentials responsive to said authentication
8 request so as to authenticate with the first security realm;
9 means for accessing a second resource in the first security realm; and
10 responsive to said accessing the second resource, means for automatically
11 authenticating with a second security realm.

1 22. (Original) The apparatus of claim 21, further comprising:
2 means for displaying a logout element within the web browser for performing said
3 automatically authenticating with the second security realm; and
4 within a single browser session:
5 means for authenticating a first user with the first security realm;
6 means for authenticating the first user with the second security realm so
7 as to de-authenticate the first user from the first security realm; and
8 means for authenticating a second user with the first security realm.
9

10 23. (New) A de-authentication method for a web browser, comprising:

11 accessing a first resource of a first security realm of the web server with the web
12 browser, the web browser operable to automatically cache authentication credentials for
13 a current security realm to which the web browser is authenticated;

14 receiving a request for authentication responsive to requesting the first resource;

15 authenticating with the first security realm based at least in part on providing
16 authentication credentials responsive to the request for authentication, so that the
17 current security realm is first security realm; and

18 de-authenticating from the first web server security realm based at least in part
19 on accessing a second resource of a second security realm different from the first
20 resource of the first security realm, so that the current security realm changes from the
21 first security realm to the second security realm.

22
23 24. (New) The method of claim 23, wherein the web browser and the web
24 server communicate using a stateless communication protocol.